Fortra Completes Investigation Into GoAnywhere Zero-Day Incident

Fortra has completed the investigation into the recent zero-day incident involving its GoAnywhere managed file transfer (MFT) software and the company has shared a summary of its findings.

The investigation, conducted with the aid of cybersecurity firm Palo Alto Networks, revealed that malicious activity started on January 18, with cybercriminals exploiting a zero-day vulnerability against on-premises implementations running a specific configuration of GoAnywhere.

In the case of MFTaaS customers, the probe found that they were targeted with the zero-day vulnerability starting with January 28.

Fortra became aware of the hack on January 30 and the unauthorized activity conducted in MFTaaS environments was completely neutralized the next day. The zero-day vulnerability, tracked as CVE-2023-0669, can be exploited for remote code execution.

“Our initial investigation revealed the unauthorized party used CVE-2023-0669 to create unauthorized user accounts in some MFTaaS customer environments. For a subset of these customers, the unauthorized party leveraged these user accounts to download files from their hosted MFTaaS environments,” the company explained.

In addition, the attackers leveraged the zero-day to install

up to two tools in compromised customer environments: Netcat and Errors.jsp.

Fortra said it immediately started working with customers to resolve the breach, but a patch for the zero-day was only released roughly one week after the incident was made public.

“At this time, we can confirm this issue was isolated to our GoAnywhere MFT solution and does not involve any other aspects of the Fortra business, or its customers,” Fortra said.

The company has also described the actions it has taken to prevent future incidents and shared some recommendations for customers.

The zero-day vulnerability appears to have been exploited by hackers associated with the Cl0p ransomware operation.

Dozens have been impacted and several major organizations have confirmed being hit, including Community Health Systems (CHS), Rubrik, Hitachi Energy, Crown Resorts, the City of Toronto, Saks Fifth Avenue, Pluralsight, PPF, P&G, Atos, and Rio Tinto. The hackers claimed that they targeted 130 organizations in the GoAnywhere campaign.

Several victims said that while the attackers did exploit the vulnerability against them, impact was limited. Files allegedly stolen from some of them have been published on Cl0p’s leak website.

Related: Data Breach at Independent Living Systems Impacts 4 Million Individuals

Related: Western Digital Shuts Down Services Due to Cybersecurity Breach

Related: Latitude Financial Services Data Breach Impacts 300,000 Customers

https://www.securityweek.com/fortra-completes-investigation-in

to-goanywhere-zero-day-incident/